

DETAILED ACTION

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it **MUST** be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Kevin J. Zilka Reg. No. 41,429 on 4/25/2008.

2. The application has been amended as follows:

Claim 1 (Currently Amended) A computer program product embodied on a tangible computer readable medium for controlling a computer to generate mobile computing device malware definition data for use by a mobile computing device malware scanner executable upon a mobile computing device, said computer program product comprising:

obtaining code operable to obtain from a data source master malware definition data, said master malware definition identifying a plurality of items of malware each belonging to one of a plurality of classes of malware threat;

identifying code operable to identify one or more classes of malware threat against which said mobile computing device is to be protected; and

generating code operable to generate from said master malware definition data said mobile computing device malware definition data, said mobile computing device

Art Unit: 2132

malware definition data identifying items of malware identified within said master malware definition data which are within classes of malware threat against which said mobile computing device is to be protected;

wherein said obtaining code, said identifying code and said generating code are executed by a fixed location computing device, said fixed location computer being operable to transfer to said mobile computing device one or more computer files including at least, a computer file containing said mobile computer device malware definition data;

wherein said fixed location computing device stores profile data identifying one or more different types of mobile computing device to which said fixed location computing device transfers computer files and corresponding threat data identifying one or more classes of malware threat to which each of said mobile computing devices is vulnerable;

wherein only a subset of said master malware definition data is used to generate said mobile computing device malware definition data for tailoring said mobile computing device malware definition data to accommodate malware threats to which said mobile computing device is vulnerable; wherein said one or more classes of malware threat against which said mobile computing device is to be protected are chosen according to classes of malware threat known to pose a problem to said mobile computing device, and classes for which it is desired to protect said mobile computing device according to user defined policies;

wherein fixed location computing device also transfers a malware scanner computer program from said data source to said mobile computing device; and wherein said fixed

Art Unit: 2132

location computing device checks for an updated malware scanner computer program becoming available from said data source and, if such an updated malware scanner computer program become available, then obtains said updated malware scanner computer program for transfer to said mobile computing device.

Claim11 (Canceled)

Claim 13 (Canceled)

Claim17 (Currently Amended) A method of generating mobile computing device malware definition data for use by a mobile computing device malware scanner executable upon a mobile computing device, said method comprising the steps of: obtaining from a data source master malware definition data, said master malware definition identifying a plurality of items of malware each belonging to one of a plurality of classes of malware threat; identifying one or more classes of malware threat against which said mobile computing device is to be protected; and generating from said master malware definition data said mobile computing device malware definition data, said mobile computing device malware definition data identifying items of malware identified within said master malware definition data which are within classes of malware threat against which said mobile computing device is to be protected; wherein said steps of obtaining, identifying and generating are performed by a fixed location computing device, said fixed location computer being operable to transfer to

said mobile computing device one or more computer files including at least a computer file containing said mobile computer device malware definition data;

wherein said fixed location computing device stores profile data identifying one or more different types of mobile computing device to which said fixed location computing device transfers computer files and corresponding threat data identifying one or more classes of malware threat to which each of said mobile computing devices is vulnerable;

wherein only a subset of said master malware definition data is used to generate said mobile computing device malware definition data for tailoring said mobile computing device malware definition data to accommodate malware threats to which said mobile computing device is vulnerable;

wherein fixed location computing device also transfers a malware scanner computer program from said data source to said mobile computing device; and wherein said fixed location computing device checks for an updated malware scanner computer program becoming available from said data source and, if such an updated malware scanner computer program become available, then obtains said updated malware scanner computer program for transfer to said mobile computing device.

Claim 27 (Canceled)

Claim 29 (Canceled)

Claim 33 (Currently Amended) Apparatus for generating mobile computing device malware definition data for use by a mobile computing device malware scanner executable upon a mobile computing device, said apparatus comprising:

obtaining logic operable to obtain from a data source master malware definition data, said master malware definition identifying a plurality of items of malware each belonging to one of a plurality of classes of malware threat;

identifying logic operable to identify one or more classes of malware threat against which said mobile computing device is to be protected; and

generating logic operable to generate from said master malware definition data said mobile computing device malware definition data, said mobile computing device malware definition data identifying items of malware identified within said master malware definition data which are within classes of malware threat against which said mobile computing device is to be protected;

wherein said obtaining logic, said identifying logic and said generating logic are provided by a fixed location computing device, said fixed location computer being operable to transfer to said mobile computing device one or more computer files including at least a computer file containing said mobile computer device malware definition data;

wherein said fixed location computing device stores profile data identifying one or more different types of mobile computing device to which said fixed location computing device transfers computer files and corresponding threat data identifying one or more classes of malware threat to which each of said mobile computing devices is vulnerable;

wherein only a subset of said master malware definition data is used to generate said mobile computing device malware definition data for tailoring said mobile computing device malware definition data to accommodate malware threats to which said mobile

Art Unit: 2132

computing device is vulnerable; wherein fixed location computing device also transfers a malware scanner computer program from said data source to said mobile computing device; and wherein said fixed location computing device checks for an updated malware scanner computer program becoming available from said data source and, if such an updated malware scanner computer program become available, then obtains said updated malware scanner computer program for transfer to said mobile computing device.

Claim 43 (Canceled)

Claim 45 (Canceled)

3. The following is an examiner's statement of reasons for allowance:

As noted on page 24 (Group #6), the cited references of Nambu (20020124181) and Hershberg et al. (20030022657) do not teach or suggest the specific feature of a fixed location computing device transferring a malware scanner computer program from said data source to said mobile computing device; and wherein said fixed location computing device checks for an updated malware scanner computer program becoming available from said data source and, if such an updated malware scanner computer program become available, then obtains said updated malware scanner computer program for transfer to said mobile computing device.

4. Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Art Unit: 2132

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to SAOUSSEN BESROUR whose telephone number is (571)272-6547. The examiner can normally be reached on M-F 8:30am to 5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/S. B./

Examiner, Art Unit 2131

April 25, 2008

/Gilberto Barron Jr/

Supervisory Patent Examiner, Art Unit 2132